JOHNSON LAMBERT

Insurance Topics

New York on the Cusp of Adopting Cybersecurity Regulations

January 2017

Insurance companies and other organizations regulated by the New York State Department of Financial Services (NYDFS) will soon be subject to cybersecurity regulations. The NYDFS published the second draft of its proposed regulations in the New York State Register on 12.28.16. The proposal is subject to a final 30-day comment period and is expected to be effective 03.01.17. The proposal is the first of its kind.

The following table summarizes the key provisions of the cybersecurity regulations, which is predicated on an entity performing a risk assessment and using the results of that assessment to drive the development and maintenance of its cybersecurity program.

Section	Summary	Compliance Period
500.02 Cybersecurity Program	Implement a cybersecurity program that: • Identifies and assesses internal and external cyber risks • Uses defensive infrastructure to protect from unauthorized access, use or malicious acts • Detects, responds to and recovers from cybersecurity events • Fulfills regulatory reporting requirements	180 days from the effective date
500.03 Cybersecurity Policy	Maintain written cybersecurity policies and procedures, based on the entity's risk assessment, that are approved by a Senior Officer, the Board of Directors or equivalent governing body.	180 days from the effective date
500.04 Chief Information Security Officer	Designate a qualified individual (employee, affiliate or third party service provider) responsible for overseeing the cybersecurity program and reporting the following to the Senior Officer, Board of Directors or equivalent governing body annually: • Assessment of the confidentiality of nonpublic information (NPI) and the integrity and security of the entity's information systems (IS) • Material cyber risks to the entity • Material cybersecurity events involving the entity during the reporting period • Assessment of the overall effectiveness of the cybersecurity program	Designating a qualified individual- 180 days from the effective date Reporting - One year from the effective date
500.05 Penetration Testing and Vulnerability Assessments	Conduct monitoring and testing to assess the effectiveness of the cybersecurity program, based on the entity's risk assessment. Continuous monitoring or periodic penetration and vulnerability assessments should be performed. If continuous monitoring, or an equivalent control to identify changes that may create or increase vulnerabilities, is not feasible, an entity must conduct: • Annual penetration testing • Bi-annual vulnerability assessments	One year from the effective date
500.06 Audit Trail	Maintain the following for no less than five years: • Records allowing the reconstruction of material financial transactions to support normal operations • Audit trails that detect and respond to cybersecurity events that are reasonably likely to materially harm material components of normal operations	18 months from the effective date
500.07 Access Privileges	User access to IS should be limited and periodically reviewed to ensure such access is appropriate.	180 days from the effective date
500.08 Application Security	Document procedures regarding: • Secure development practices for internally developed software • Evaluating or testing the security of externally developed applications Such documentation must be periodically reviewed by the Chief Information Security Officer (CISO) or equivalent.	18 months from the effective date

Section	Summary	Compliance Period
500.09 Risk Assessment	Conduct periodic risk assessments to design the cybersecurity program and address changes to the IS, NPI or business operations. The cybersecurity program should be updated, as needed, to respond to the results of the risk assessments.	One year from the effective date
500.10 Cybersecurity Personnel and Intelligence	Qualified personnel (employees, affiliates or third party service providers) must be utilized to manage, perform and oversee the entity's cybersecurity program. Such personnel should receive cybersecurity updates and training. An entity must verify that key cybersecurity personnel have current knowledge of cybersecurity threats and countermeasures.	180 days from the effective date
500.11 Third Party Service Provider Security Policy	Document policies and procedures regarding: • Identification, risk assessments (initial and subsequent) and selection of third party service providers • Cybersecurity requirements to be met by the third party service providers (should equal to or exceed the requirements imposed by the cybersecurity regulations) • Periodic due diligence testing over the adequacy of the cybersecurity practices of the third party services provider	Two years from the effective date
500.12 Multi-Factor Authentication	Establish controls to protect against unauthorized access to NPI or IS. Such controls may include multi-factor authentication, risk-based authentication or reasonably equivalent controls approved by the CISO or equivalent.	One year from the effective date
500.13 Limitations on Data Retention	Develop policies and procedures for the periodic, secure disposal of NPI that is no longer required for business operations or other legitimate purposes (e.g. retention is required by law or regulation).	18 months from the effective date
500.14 Training and Monitoring	Develop policies, procedures and controls to monitor authorized user activity and detect unauthorized access to and use of NPI. Provide cybersecurity awareness training for all personnel.	Monitoring - 18 months from the effective date Training - One year from the effective date
500.15 Encryption of Nonpublic Information	Implement encryption controls over NPI held and transmitted by the entity. When encryption is not feasbile, the CISO or equivalent may approve alternate compensating controls. The CISO or equivalent must evaluate the feasibility of encryption and the compensating controls no less than annually.	18 months from the effective date
500.16 Incident Response Plan	Implement a written incident response plan to respond to and recover from cybersecurity events that materially affect the IS or the ability of the entity to continue its business operations.	180 days from the effective date

Section	Summary	Compliance Period
500.17 Notices to Superintendent	Notify the NYDFS Superintendent within 72 hours of any cybersecurity event that has a reasonable likelihood of materially harming a material part of the entity's normal operations or is otherwise required to be reported to a government body, self-regulatory agency or other supervisory body. Annual certification of compliance with the cybersecurity regulation must be submitted by February 15.	180 days from the effective date
500.18 Confidentiality	Information provided in compliance with this cybersecurity regulation is exempt from disclosure under the Baking Law, Insurance Law, Financial Services Law, Public Officers Law or other applicable federal or state law.	N/A
500.19 Exemptions	The following are exempt from this regulation: • Entities with fewer than 10 employees, including independent contractors • Entities with less than $5,000,000 in gross annual revenue in each of the last three fiscal years • Entities with less than $10,000,000 in year-end total assets, calculated in accordance with GAAP, including affiliate assets • Employees, agents, representatives or designees of the covered entity who meet the definition of "covered entity" but are covered by an entity's cybersecurity program • Entities that do not directly or indirectly maintain or oversee access to IS or NPI.	N/A

The full text of the regulations can be found here.

If you have any questions regarding the impact of these regulations on your entity, please contact Kim Mobley, CPA, Partner at kmobley@johnsonlambert.com.